Deutscher Bundestag **Drucksache 19/8650**
19. Wahlperiode 22.03.2019

Kleine Anfrage

der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Espendiller und der Fraktion der AfD

Sicherstellung der technischen Integrität der künftigen 5G-Mobilfunkinfrastruktur

Laut Medienberichten gab es Anfang Februar 2019 (www.handelsblatt.com/politik/deutschland/5g-ausbau-bnd-und-auswaertiges-amt-warnen-vor-chinas-macht-ueber-huawei/23991388.html) Treffen der außen-, wirtschafts- und digitalpolitischen Obleute des Deutschen Bundestages mit verschiedenen Bundesbehörden, darunter insbesondere der Bundesnachrichtendienst (BND), in denen aktuelle Erkenntnisse über sicherheitsrelevante Informationen über den Aufbau des künftigen 5G-Mobilfunknetzes in Deutschland präsentiert wurden.

Weitere Informationen sollen Regierungsbeamten, Parlamentariern und ausgewählten Empfängern in Form eines Papiers des Mercator Institute for China Studies (MERICS) vorgelegt worden sein (www.handelsblatt.com/politik/deutschland/huawei-konflikt-studie-zu-5g-warnt-vor-chinesischer-netzwerktechnologie/24024110.html).

Wir fragen die Bundesregierung:

1. Liegen der Bundesregierung, insbesondere durch Informationen des BND oder auch anderer nachgeordneter Behörden, Informationen über einen konkreten Sicherheitsvorfall („smoking gun“) mit Huawei-Hardware vor?
2. Liegen dem Bundesnachrichtendienst nähere Informationen zu den NSA-Operationen „Parody Blowup“ oder „Shotgiant“ aus den Jahren 2006 und 2009 vor, die Huawei als „einzigartige Bedrohung“ beschreiben (www.zeit.de/2019/09/huawei-mobiles-internet-5g-china-spionageverdacht-konzern)?
3. Welche Schlussfolgerungen zieht die Bundesregierung aus der Einschätzung des Mercator Institute for China Studies (MERICS), dass sich weder Huawei noch andere chinesische Konzerne dem Einfluss des chinesischen Staates, insbesondere auf Basis des am 1. Mai 2015 in Kraft getretenen Staatssicherheitsgesetzes, aus Gründen der Nationalen Sicherheit entziehen können (www.golem.de/news/huawei-wartungsschnittstellen-sind-keine-hintertueren-1902-139554.html)?
4. Welche Schlussfolgerungen zieht die Bundesregierung aus der Einschätzung des Mercator Institute for China Studies (MERICS), dass auch die tatsächliche Rechts- und Verwaltungspraxis in China nicht dafür spricht, im Bereich kritische Infrastruktur und Daten vertrauensvoll mit chinesischen Unternehmen zusammenarbeiten zu können (www.golem.de/news/huawei-wartungsschnittstellen-sind-keine-hintertueren-1902-139554.html)?

5. Priorisiert die Bundesregierung entweder einen schnellen Ausbau des 5G-Mobilfunknetzes in Deutschland oder die Verwendung sicherer Soft- und Hardwarekomponenten, welche Gründe legt die Bundesregierung ihrer Entscheidung zugrunde, und welche Folgerungen ergeben sich aus dieser Priorisierung für die Bundesregierung?
6. Mit welchen zusätzlichen Kosten für den Aufbau der 5G-Infrastruktur rechnet die Bundesregierung bei einem Ausschluss von Huawei und dem Ersatz von Huawei-Produkten durch andere Hersteller?
7. Nach welchen spezifischen Kriterien des Katalogs von Sicherheitsanforderungen nach § 109 des Telekommunikationsgesetzes (TKG) beabsichtigt die Bundesregierung die geplante Vertrauenswürdigkeitsprüfung von Hersteller-„Ländern“ durchzuführen, und welche weiteren Kriterien sollen im Rahmen der geplanten Gesetzesänderung des TKG (www.golem.de/news/tkg-aenderung-regierung-plant-angeblich-knebelgesetz-fuer-huawei-1902-139360.html) dazu noch in den § 109 aufgenommen werden?
8. In welcher Form soll die in dem Antrag der Fraktion der AfD „Schutz der Kritischen 5G-Infrastruktur vor staatsnahen Netzwerkausrüstern“ (Bundestagsdrucksache 19/7723) aufgestellte Forderung nach einer Beweislastumkehr für Netzwerkausrüster gesetzgeberisch und exekutiv umgesetzt werden, und bis wann?
9. Werden derzeit durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder andere Bundesbehörden im Rahmen von Zertifizierungsverfahren kontinuierliche und vollumfängliche Prüfungen sämtlicher Hard- und Software-Updates für 2G-, 3G- und 4G-Netze durchgeführt?

   Wenn nein, warum nicht?
10. Sind solche kontinuierlichen und vollumfänglichen Prüfungen sämtlicher Hard- und Software-Updates im Rahmen von Zertifizierungsverfahren auch für das 5G-Netz geplant?
11. Hält die Bundesregierung die in dem Antrag der Fraktion der AfD „Schutz der Kritischen 5G-Infrastruktur vor staatsnahen Netzwerkausrüstern“ (Bundestagsdrucksache 19/7723) aufgestellte Forderung, das „BSI mit entsprechenden Ressourcen auszustatten, sämtliche Programmecode-Updates vor deren Installation umfassend zu prüfen und zu zertifizieren“, für realistisch und zielführend, und wird die Bundesregierung diese Forderung umsetzen?
12. Wie bewertet die Bundesregierung die Aussage des BSI-Präsidenten Arne Schönbohm, das BSI könne jedes einzelne von Huawei verbaute Gerät und jedes Software-Update vor Inbetriebnahme prüfen, (www.zeit.de/2019/09/huawei-mobiles-internet-5g-china-spionageverdacht-konzern) im Hinblick auf ihre Umsetzbarkeit?
13. Wie viele von Huawei verbaute Geräte und wie viele Software-Updates pro Zeiteinheit legt BSI-Präsident Arne Schönbohm dieser Aussage zugrunde?
14. Welche personellen (bitte Anzahl der Personalstellen in Vollzeitäquivalenten angeben), technischen (bitte Anzahl Laborgeräte, Server etc. angeben), finanziellen (bitte in Tausend Euro angeben) und organisatorischen (bitte Konzepte zur Organisationsgestaltung, z. B. in Form einer besonderen Aufbauorganisation – BAO –, Verantwortlichkeiten, Prüfabläufen etc. angeben) Voraussetzungen sind für die Umsetzung der von BSI-Präsident Schönbohm angekündigten Huawei-Prüfungen erforderlich, und bis wann, und in welchem Aufwuchszeitraum (bitte in Personenmonaten angeben) können diese Voraussetzungen geschaffen werden?

15. Sieht die Bundesregierung Handlungsbedarf hinsichtlich einer EU-rechtlichen Harmonisierung des § 109 TKG, um eine einheitliche Rechtsgrundlage für ein konsolidiertes europäisches Vorgehen zum Schutz kritischer Telekommunikationsinfrastrukturen zu schaffen?

    Wenn nein, warum nicht?

16. Welche Möglichkeiten sieht die Bundesregierung, EU-Champions als Hersteller von Hard- und Softwarekomponenten von KRITIS-Infrastruktur oder die Ansiedlung von Produktionskapazitäten außereuropäischer Hardware- und Softwarehersteller in Deutschland oder Europa zu fördern, um eine weitgehend EU-autarke Versorgung zu gewährleisten?

    a) Welches Finanzvolumen wäre nach Meinung der Bundesregierung für eine solche Förderung notwendig?

    b) Welcher Zeitraum wäre nach Meinung der Bundesregierung für eine solche Förderung notwendig?

17. Hält die Bundesregierung die in dem Antrag der Fraktion der AfD „Schutz der Kritischen 5G-Infrastruktur vor staatsnahen Netzwerkausrüstern“ (Bundestagsdrucksache 19/7723) aufgestellte Forderung, „im Bereich der noch verbleibenden Standardisierung von 5G, insbesondere im Rahmen des Third Generation Partnership Projects (3GPP), bis zum Jahr 2020 zusätzliche öffentliche Mittel zu veranschlagen, um die Wahrnehmung deutscher Interessen in internationalen Standardisierungsgremien insbesondere im Bereich der Netzwerksicherheit zu gewährleisten“, für realistisch und zielführend, und wird die Bundesregierung diese Forderung umsetzen?

18. Wie bewertet die Bundesregierung die in dem Antrag der Fraktion der AfD „Schutz der Kritischen 5G-Infrastruktur vor staatsnahen Netzwerkausrüstern“ (Bundestagsdrucksache 19/7723) aufgestellte Forderung, „bestehende Möglichkeiten der Ende-zu-Ende-Verschlüsselung auf Anwendungsebene zu bewahren und auszubauen, da sie ein hohes Maß an Sicherheit gewährleisten und für die Nutzer ferner transparent und nachvollziehbar sind“, und wird die Bundesregierung diese Forderung umsetzen?

19. Welche Sicherheitsrisiken sieht die Bundesregierung durch den Einsatz von Hardware- und Softwarekomponenten nichteuropäischer Hersteller auch im Bereich der Festnetzinfrastruktur, und welcher akute und strategische Handlungsbedarf folgt für die Bundesregierung aus dieser Risikobewertung?

Berlin, den 26. Februar 2019

Dr. Alice Weidel, Dr. Alexander Gauland und Fraktion



Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333